Camera Cell Phones in the Workplace – Get the Picture!

written by Rory Lodge | April 16, 2014

Beware. A new technology is gaining popularity in the United States which may potentially pose a threat, particularly to healthcare employers. The technology is the camera cell phone. If you think that this emerging technology should not be a concern, think again.

Proprietary Information

Camera phones pose a substantial threat to a business privacy, confidentiality and proprietary interests. Camera phones are the same size and of the same appearance as regular cell phones, making them virtually indistinguishable. The phones can be used to snap photos while the user appears to be making a call. The candid shots can then be e-mailed to others or transmitted almost instantaneously to a website. And, the alleged saboteur need not smuggle a camera and film outside of the facility in order to do so. While this may sound like a scene from a James Bond movie, the repercussions for a healthcare facility can be severe.

Most businesses spend substantial time and money protecting their proprietary information. Employees, visitors and others are prohibited from photocopying or recording sensitive and confidential information and accessing computer networks. With a camera cell phone, a visitor could easily, and inconspicuously, breach these security measures by taking pictures of internal memos, employee files, patient records and financial records, to name a few. However, visitors are not the only culprits to be feared. Think of the harm that a disgruntled employee, patient or family member could cause with the indiscreet use of a camera phone. Your proprietary and other confidential information could easily and quickly fall into the hands of a competitor, a regulator, or worse, those with dishonorable intentions.

Privacy Concerns

With cubicle office designs being commonplace, co-workers could easily snap candid photos of fellow workers at the office. Moreover, the cameras could easily be taken into a locker room or restroom. The candid photos then could be sent through your e-

mail or be transmitted over the internet. If the photograph happens to be of an employee in a compromising situation, a sexual harassment suit could quickly ensue.

Please don't think that your employees are above such adolescent behavior. In Japan, for instance, several men have been caught snapping pictures up women's skirts. Others have been apprehended secretly taking photos down into bathroom stalls. There's no reason to assume that this is not occurring elsewhere. In response to this type of behavior, Japan's camera phones are now designed to set off an electronic ring or click when the shutter is pressed, thereby warning everybody nearby that a photograph is being taken. This technology has not yet become commonplace on our side of the Pacific.

In the United States, several health clubs have placed restrictions on the use of camera phones in response to privacy concerns. Some clubs limit the use of camera phones to the lobby while others completely ban the use of camera phones on the premises.

Healthcare facilities also present obvious privacy issues concerning our patients and residents and their records. The individuals we are caring for have, and indeed are entitled to, an expectation of privacy in most areas of our facilities, not necessarily limited to their rooms. Their records are also subject to privacy and confidentiality concerns, not the least of which is HIPPA. Once again, a visitor, employee or even a patient could create serious issues through unauthorized use of a camera phone.

How You Can Protect Yourself

To properly protect your facility, you must be proactive. If you haven't already done so, now is the best time to establish a policy concerning camera phones or cell phones in general. Consider revising your employee handbook to address the privacy and proprietary concerns of camera phones in the workplace. If the policy will also apply to visitors and others having access to your facility, which it should, the policy should be clearly posted at facility entrances. Consider also policy limitations on your patients, residents and their families. However, prior to establishing a "take no prisoners" policy which may not be well received by patients, employees or visitors, you should conduct a vulnerability assessment. What are your proprietary concerns? Privacy? Confidentiality? Will the policy apply to employees? Visitors? Patients? Residents? Others? Should there be different policies or policy limitations for each? To which locations inside the facility should the policy apply? How will you publicize the policy? Who will enforce the policy? Are there areas within your facility where camera phone use may be acceptable? Will the policy apply to all cell phones or to camera phones only?

After analyzing the risks, you should take the necessary steps to enact a policy or policies which meet your needs. The policy could be as restrictive as an outright ban of camera phones or it could ban camera phones from only sensitive areas, including patient rooms, record rooms, restrooms and locker rooms. If cell phones are provided to any of your employees or if you pay an employee's cell phone bill, the policy could dictate that camera phones will not be provided or that the employer will not pay for an employee's use of a camera phone.

Several businesses have already enacted camera phone policies. For instance, Daimler Chrysler prohibits employees and visitors from bringing camera phones into any company building, while Texas Instruments permits camera phones at work, but forbids them to be used to take pictures. Samsung Electronics requires employees and visitors to stick tape over the handset's camera lens. These policies are merely examples of how businesses are trying to cope with this new problem. That said, each healthcare

facility should enact a policy that meets its own particular business and confidentiality needs and should do so promptly.

by John E. Lyncheski and Lisa L. Garrett